



Book	Policy Manual
Section	READY FOR 7-14-26
Title	Copy of STAFF AND SCHOOL OFFICIALS USE OF PERSONAL COMMUNICATION DEVICES
Code	po7530.02
Status	
Adopted	December 8, 2015
Last Revised	July 14, 2026
Prior Revised Dates	10/14/2025

7530.02 - **STAFF AND SCHOOL OFFICIALS USE OF PERSONAL COMMUNICATION DEVICES**

Use of personal communication devices ("PCD") (as defined in Bylaw 0100 - Definitions) has become pervasive in the workplace. Whether the PCD is Board-owned and assigned to a specific employee or school official or personally-owned by the employee or school official regardless of whether the Board pays the employee or school official an allowance for their use of the device, the Board reimburses the employee or school official on a per-use basis for their business-related use of their PCD, or the employee or school official receives no remuneration for their use of a personally-owned PCD, the employee or school official is responsible for using the device in a safe and appropriate manner and in accordance with this policy and its accompanying guideline, as well as other pertinent Board policies and guidelines.

District-Approved PCD Platform - When communicating with students, Board members, staff, coaches/advisors, and approved volunteers are required to exclusively use the District-approved social media/communication platforms/sites. See Policy 1213/3213/4213 - Student Supervision and Welfare for specifics regarding appropriate discussion content when using PCDs as well as the approved PCD Platform.

Conducting District Business Using a PCD

Employees and school officials are responsible for archiving such communication(s) in accordance with the District's requirements.

Individuals are responsible for retaining text messages, instant messages, and other written communications that are not archived by the District; such records shall be retained in accordance with State requirements.

Safe and Appropriate Use of a PCD

Employees and school officials are responsible for operating Board-owned vehicles and potentially hazardous equipment in a safe and prudent manner, and therefore, employees are prohibited from using PCDs while operating such vehicles or equipment. In the interest of safety for both Board employees and other drivers, employees are required to comply with all applicable laws while driving.

Employees and school officials may not use a PCD in a way that might reasonably create in the mind of another person an impression of being threatened, humiliated, harassed, embarrassed, or intimidated.

Duty to Maintain Confidentiality of Student Personally Identifiable Information - Public and Student Record Requirements

Employees and school officials are subject to all applicable policies and guidelines pertaining to the protection of the security, integrity, and availability of the data stored on a PCD, regardless of whether they are Board-owned and assigned to a specific employee or personally-owned by the employee.

PCD communications, including calls, text messages, instant messages, and e-mails sent or received, may not be secure. Therefore, employees should use discretion when using a PCD to relay confidential information, particularly as it relates to students.

Additionally, PCD communications, including text messages, instant messages, and e-mails sent and/or received by a public employee or school official using a PCD, may constitute public records.

Further, PCD communications about students, including text messages, instant messages, and e-mails sent and/or received by a District employee or school official using their PCD, may constitute education records if the content includes personally identifiable information about a student.

Communications, including text messages, instant messages, and e-mails sent and/or received by a District employee or school official using their PCD, that are public records or student records are subject to retention and disclosure, upon request, in accordance with Policy 8310 - Public Records. Cellular/Wireless communications that are student records should be maintained pursuant to Policy 8330 - Student Records.

It is the responsibility of the District employee or school official who uses a PCD for District business-related use to archive all text messages, instant messages, and e-mails sent and/or received using their PCD in accordance with the District's requirements.

Cellular/Wireless communications and other electronically stored information (ESI) stored on the staff member's or school official's PCD may be subject to a litigation hold pursuant to Policy 8315 - Information Management. Staff and school officials are required to comply with District requests to produce copies of cellular/wireless communications in their possession that are either public records or education records or that constitute ESI that is subject to a litigation hold.

~~Employees and school officials are subject to all applicable policies and guidelines pertaining to the protection of the security, integrity, and availability of the data stored on a PCD, regardless of whether they are Board-owned and assigned to a specific employee or personally-owned by the employee.~~

~~PCD communications, including calls, text messages, instant messages, and e-mails sent or received, may not be secure. Therefore, employees should use discretion when using a PCD to relay confidential information, particularly as it relates to students.~~

~~Additionally, PCD communications, including text messages, instant messages, and e-mails sent and/or received by a public employee or school official using a PCD, may constitute public records.~~

~~Further, PCD communications about students, including text messages, instant messages, and e-mails sent and/or received by a District employee or school official using their PCD, may constitute education records if the content includes personally identifiable information about a student.~~

~~Communications, including text messages, instant messages, and e-mails sent and/or received by a District employee or school official using their PCD, that are public records or student records are subject to retention and disclosure, upon request, in accordance with Policy 8310 - Public Records. Cellular/Wireless communications that are student records should be maintained pursuant to Policy 8330 - Student Records.~~

~~It is the responsibility of the District employee or school official who uses a PCD for District business-related use to archive all text messages, instant messages, and e-mails sent and/or received using their PCD in accordance with the District's requirements.~~

~~Cellular/Wireless communications and other electronically stored information (ESI) stored on the staff member's or school official's PCD may be subject to a litigation hold pursuant to Policy 8315 - Information Management. Staff and school officials are required to comply with District requests to produce copies of cellular/wireless communications in their possession that are either public records or education records or that constitute ESI that is subject to a litigation hold.~~

If a PCD is lost, stolen, hacked, or otherwise subjected to unauthorized access, the employee or school official must immediately notify the District Administrator so a determination can be made as to whether any public records, student records, and/or ESI subject to a litigation hold has been compromised and/or lost. Pursuant to Policy 8305 - Information Security and its accompanying guideline, the District Administrator shall determine whether any security breach notification

laws may have application to the situation. Appropriate notifications will be sent unless the records/information stored on the PCD was encrypted.

The Board prohibits employees and school officials from maintaining the following types of student, staff, or District records and/or information on their PCDs:

- A. social security numbers
- B. driver's license numbers
- C. credit and debit card information
- D. financial account numbers
- E. student personally identifiable information
- F. information required to be kept confidential pursuant to the Americans with Disabilities Act (ADA)
- G. personal health information as defined by the Health Insurance Portability and Accountability Act (HIPAA)

It is suggested that employees and school officials lock and password-protect their PCDs when not in use.

Employees and school officials are responsible for making sure no third parties (including family members) have access to records and/or information, which is maintained on a PCD in their possession, that is confidential, privileged, or otherwise protected by State and/or Federal law.

Privacy Issues

Except in emergency situations or as otherwise authorized by the District Administrator or as necessary to fulfill their job responsibilities, employees are prohibited from using PCDs to capture, record and/or transmit the words or sounds (i.e., audio) and/or images (i.e., pictures/video) of any student, staff member or other person in the school or while attending a school-related activity. Using a PCD to capture, record, and/or transmit audio and/or pictures/video of an individual without proper consent is considered an invasion of privacy and is not permitted.

PCDs, including but not limited to those with cameras, may not be activated or utilized at any time in any school situation where a reasonable expectation of personal privacy exists. These locations and circumstances include, but are not limited to, classrooms, gymnasiums, locker rooms, shower facilities, rest/bathrooms, and any other areas where students or others may change clothes or be in any stage or degree of disrobing or changing clothes. The District Administrator and building principals are authorized to determine other specific locations and situations where use of a PCD is absolutely prohibited.

Personal Use of PCDs While at Work

During work hours, personal communications made or received, regardless of whether on a PCD or a regular telephone, or a network computer, can interfere with employee productivity and distract others. Employees are expected to use discretion in using PCDs while at work for personal business. Employees are asked to limit personal communications to breaks and lunch periods, and to inform friends and family members of the Board's policy in this regard.

Potential Disciplinary Action

Violation of this policy may ~~result in~~ constitute just cause for disciplinary action, up to and including termination. Use of a PCD in any manner contrary to local, State, or Federal laws may also result in disciplinary action up to and including termination.

Use of a PCD in any manner contrary to local, State, or Federal laws may also result in disciplinary action up to and including termination.

Protecting Children in the 21st Century Act, Pub. L. No. 110-385, Title II, Stat. 4096 (2008)
Children's Internet Protection Act (CIPA), Pub. L. No. 106-554 (2001)
20 U.S.C. 1232g
34 C.F.R. Part 99

118.07(7), Wis. Stats.

948.072, Wis. Stats.

© Neola 202526

Legal Protecting Children in the 21st Century Act, Pub. L. No. 110-385, Title II, Stat. 4096 (2008)

Cross References Children's Internet Protection Act (CIPA), Pub. L. No. 106-554 (2001)
20 U.S.C. 1232g
34 C.F.R. Part 99
118.07(7), Wis. Stats.
948.072, Wis. Stats.

Last Modified by Coleen Frisch on June 30, 2026